

March   , 2020

Sample  
123 Main St  
City, State Zip

***RE: Important Security Notification. Please read this entire letter.***

Dear Sir or Madam:

We are writing to inform you of an incident that may affect the security of your personal information. We take this incident very seriously and are providing you with information, as well as access to resources, so that you can better protect against the possibility of misuse of your personal information.

**What Happened:**

On or around September 17, 2019, Athens Insurance Services, Inc. (“Athens”) became aware of a potential compromise to one (1) of its employee’s email account. Athens immediately took actionable steps to secure the affected account, including changing the account password. Further, Athens engaged an expert forensic company to investigate the incident. It was ultimately determined that one (1) email account experienced unauthorized access between July 1, 2019 and September 17, 2019. On January 22, 2020, after thorough investigation, Athens determined that the unauthorized access may have allowed access to your personal information. Athens has worked diligently to obtain sufficient contact information to provide notification.

While we have no information to suggest that any information was misused during this compromise, and while this information may not constitute personal information under the law, we are providing this notification to you out of an abundance of caution and so that you may diligently monitor your accounts. We take great care in the security of our technology systems, and regret that this incident has occurred.

**What Information Was Involved:**

The personal information that could have been accessed by the unauthorized individual may have included your first and last name, Social Security number, date of birth, student identification number, driver’s license number, passport number, financial account number, username and password, medical diagnosis, treatment information, medical history, medical record number, prescription information, patient account number, clinical information and/or health insurance information.

**What We are Doing:**

Athens has taken every step necessary to address the incident, and is committed to fully protecting all of the information that you have entrusted to us. Upon learning of this incident, we immediately

took actionable steps to secure the affected account, which includes implementing additional security measures. We likewise retained a forensic firm to conduct a thorough investigation.

**Credit Monitoring:**

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

**What You Can Do:**

We recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please contact your financial institution. We have provided additional information below, which contains more information about steps you can take to protect yourself against fraud and identity theft.

**For More Information:**

Should you have questions or concerns regarding this matter, please do not hesitate to contact us at                     .

We value your business and sincerely apologize for this incident and regret any inconvenience it may cause you.

Sincerely,

Name

Title

## ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

**TransUnion®myTrueIdentity provides you with the following key features:**

- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- One year of unlimited access to your TransUnion® credit report and credit score.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible.<sup>1</sup>

### **How to Enroll: You can sign up online or via U.S. mail delivery**

- To enroll in this service, go to the *myTrueIdentity* website at **www.MyTrueIdentity.com** and, in the space referenced as “Enter Activation Code,” enter the 12-letter Activation Code <<**Insert Unique 12-letter Activation Code**>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode <<**Insert static 6-digit Telephone Pass Code**>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<**Enrollment Deadline**>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

### **➤ PLACE A 90-DAY FRAUD ALERT ON YOUR CREDIT FILE**

An **initial 90-day security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax, Consumer Fraud Division  
P.O. Box 105069, Atlanta, GA 30348 Phone: 1.800.525.6285  
[www.equifax.com](http://www.equifax.com)

---

<sup>1</sup> (Policy limitations and exclusions may apply.)

Experian, National Consumer Assistance  
P.O. Box 1017, Allen, TX 75013 Phone: 1.888.397.3742  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Victim Assistance Department  
P.O. Box 6790, Fullerton, CA 92834  
Phone: 1.800.680.7289  
[www.transunion.com](http://www.transunion.com)

### ➤ **PLACE A SECURITY FREEZE ON YOUR CREDIT FILE**

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report in connection with any new credit application, which will prevent them from extending credit. A security freeze generally does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting agencies. You should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report.

### ➤ **ORDER YOUR FREE ANNUAL CREDIT REPORTS**

Visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

### ➤ **MANAGE YOUR PERSONAL INFORMATION**

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with; and shredding receipts, statements, and other sensitive information. Remain vigilant by reviewing account statements and monitoring credit reports.

### ➤ **USE TOOLS FROM CREDIT PROVIDERS**

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

➤ **BE AWARE OF SUSPICIOUS ACTIVITY INVOLVING YOUR HEALTH INSURANCE**

Contact your healthcare provider if bills do not arrive when expected, and review your Explanation of Benefit forms to check for irregularities or suspicious activity. You can also contact your health insurance company to notify them of possible medical identity theft or ask for a new account number.

➤ **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. Additionally, any suspected identity theft should be reported to law enforcement, including your state Attorney General and the Federal Trade Commission.

- Visit <http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html> for general information regarding protecting your identity.
- The Federal Trade Commission has an identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information online at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft). For Mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, DC 20580.
- **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, [www.ncdoj.gov](http://www.ncdoj.gov).
- **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16<sup>th</sup> Floor, Baltimore, MD 21202, 1-888-743-0023, [www.oag.state.md.us](http://www.oag.state.md.us).
- **For New Mexico residents**, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to your employees; (v) you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit

Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting [https://files.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.